JAMES R. LANGEVIN
2D DISTRICT, RHODE ISLAND

COMMITTEE ON HOMELAND SECURITY
EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY
CHAIRMAN
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM
INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
TERRORISM, HUMAN INTELLIGENCE, ANALYSIS AND COUNTERINTELLIGENCE
TECHNICAL AND TACTICAL INTELLIGENCE

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE:
109 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225–2735
FAX: (202) 225–5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732–9400
FAX: (401) 737–2982

james.langevin@mail.house.gov
www.house.gov/langevin

The Honorable James R. Langevin
Opening Statement – "Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action"
April 25, 2007

Good afternoon and welcome to the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology hearing on the need to reduce vulnerabilities in our national critical infrastructure through investment and action. I'd like to begin by thanking the witnesses who appear before us today, and I appreciate your testimony.

I think last week was an eye opening experience for many of us up here. We learned that our federal systems and privately owned critical infrastructure are all extremely vulnerable to hacking. These vulnerabilities have significant and dangerous consequences. We learned that the federal government has little situational awareness of what is going on inside our systems. We cannot be sure how much information has been lost from our federal systems, and we have no idea if hackers are still inside our systems. And we learned that our laws are powerless to stop intruders – even the best compliance with FISMA does not make our systems more secure.

This week, we're going to continue our conversation from last week, and hear about some promising initiatives that are designed to reverse this trend of government failure. I'd like to take the opportunity to particularly thank Dr. Maughan for his service to our country in this field. Dr. Maughan is leading the cybersecurity research and development effort at the Department of Homeland Security's Science and Technology Directorate. Under his leadership, DHS S&T has funded research that has resulted in almost one dozen open-source and commercial products that provide capabilities such as:

- secure thumb drives,
- root kit detection,
- worm and distributed denial of service detection,
- defenses against phishing,
- network vulnerability assessment,
- software analysis, and
- security for process control systems.

His research and development funding is targeting the critical problems that threaten the integrity, availability, and reliability of our networks. Clearly, he plays a vital

role in securing our national cyberspace. But despite the criticality of this mission and the success of the program, I am troubled that this Administration continues its effort to do what Chairman Thompson calls "Homeland Security on the Cheap."

In the last seven years, more than 20 reports from such entities as the INFOSEC Research Council, the National Science Foundation, the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Research Council and the President's Commission on Critical Infrastructure Protection have all urged the government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities.

But look at what this Administration has done to cybersecurity and the research budget at the Department of Homeland Security. Though this program was slated to receive $22.7 million dollars in FY 2007, the actual numbers I've received from S&T show that we are only funding this program at $13 million dollars. For FY 2008, the President slashed the budget again, requesting $14.8 million dollars. This is an $8 million cut from the previous year.

Just listen to some of the important programs that are being cut or reduced in FY 2007:

- The budget for the DNSSEC program – which adds security to the Domain Name System – was reduced $670,000 dollars.

- The budget for the Secure Protocols for the Routing Infrastructure was zeroed out from its original amount of $2.4 million dollars.

- The budget for the Next Generation Cyber Security Technologies program, which addresses a variety of topic areas aimed at preventing, protecting against, detecting, responding to, and recovering from large-scale, high-impact cyber attacks was reduced $1.625 million dollars.

Now I don't know who is responsible for these cuts – Under Secretary Cohen, or Secretary Chertoff, or the White House – but reducing this funding is a serious strategic error by this Administration.

Just to understand how little we're spending for the sake of comparison, the FBI estimated in 2004 that cybercrime cost companies worldwide around $400 billion dollars. In 2005, the agency estimated that U.S. businesses lost $67 billion dollars. Of course, neither of these figures can measure the loss of federal information off of our networks, which may one day cost us our technological advantage over other nations. And those figures also don't count the potential environmental losses if a successful attack on our control systems is carried out.

I am deeply troubled by the lack of foresight that this Administration has demonstrated. These efforts are simply too important to be cut. The Homeland Security Committee is working to demonstrate the importance of R&D funding to this

Administration. In our recent authorization bill, we included a provision that would increase the funding level for the DHS cybersecurity R&D portfolio to $50 million dollars. Democratic efforts over the last several years have been endorsed by many notable cyber experts, and I appreciate all of this support.

The tools that will improve or revolutionize our security will not just appear overnight. Investment today plants seeds for the future, but it is incumbent upon the Federal government to take the leadership role in this effort. I thank the witnesses for appearing before us today and look forward to their testimony.